Amendment and Response and Examiner Interview Summary
Applicant: Francisco Corella
Serial No.: 09/483,186
Filed: January 14, 2000
Docket No.: 10001559-1/H300.126.101
Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES

IN THE CLAIMS

Please add claims 25-28.

Please amend claims 1-3, 6, 9-15, 18, and 21-24 as follows:

1. (Currently Amended) A public key infrastructure (PKI) comprising:

a subject;

a certificate authority issuing a first ~~unsigned~~ certificate to the subject, the first certificate including ~~that associates~~ a public key of the subject, ~~to~~ long-term identification information related to the subject, and meta-data related to the first certificate, wherein the first certificate is not signed by the certificate authority, the certificate authority maintaining a database of records representing issued ~~unsigned~~ certificates in which it stores a record representing the first ~~unsigned~~ certificate, wherein the issued ~~unsigned~~ certificates are valid until at least one of revoked by the certificate authority and expired; and

a verifier maintaining a hash table containing cryptographic hashes of valid ~~unsigned~~ certificates corresponding to the records stored in the database and including a cryptographic hash of the first ~~unsigned~~ certificate, wherein the subject presents the issued first ~~unsigned~~ certificate to the verifier for authentication and demonstrates that the subject has knowledge of a private key corresponding to the public key in the first~~unsigned~~ certificate.

2. (Currently Amended) The PKI of claim 1 wherein the first ~~unsigned~~ certificate includes an expiration date/time.

3. (Currently Amended) The PKI of claim 1 wherein the first ~~unsigned~~ certificate does not include an expiration date/time.

4. (Original) The PKI of claim 1 wherein the private key is stored in a smartcard accessible by the subject.

5. (Original) The PKI of claim 1 wherein the private key is stored in a secure software wallet accessible by the subject.

6. (Currently Amended) The PKI of claim 1 wherein the verifier computes the cryptographic hash of the first ~~unsigned~~ certificate with a collision-resistant hash function.

7. (Original) The PKI of claim 6 wherein the collision-resistant hash function is a SHA-1 hash function.

8. (Original) The PKI of claim 6 wherein the collision-resistant hash function is a MD5 hash function.

9. (Currently Amended) The PKI of claim 1 wherein the certificate authority and the verifier operate to revoke the first ~~unsigned~~ certificate when ~~the association of the subject's public key to~~at least a portion of the long-term identification information related to the subject ~~becomes invalid~~no longer applies to the subject.

10. (Currently Amended) The PKI of claim 91 wherein the certificate authority and the verifier perform ~~the~~a revocation protocol to revoke the first ~~unsigned~~ certificate when at least one of the private key is comprised and at least a portion of the long-term identification information related to the subject no longer applies to the subject, the revocation protocol including:

the certificate authority retrieving a record representing the first ~~unsigned~~ certificate from the database and obtaining a cryptographic hash of the first ~~unsigned~~ certificate;

the certificate authority sending a message to verifier containing the cryptographic hash of the first ~~unsigned~~ certificate and requesting that the verifier remove the corresponding cryptographic hash of the first ~~unsigned~~ certificate from its hash table;

the verifier removing the cryptographic hash of the first ~~unsigned~~ certificate from its hash table and notifying the certificate authority that it has removed the cryptographic hash of the first ~~unsigned~~ certificate from its hash table; and

the certificate authority collecting the notification sent by the verifier.

11. (Currently Amended) The PKI of claim 10 wherein the revocation protocol includes

the certificate authority marking the record of the first ~~unsigned~~ certificate in the database as being invalid, for auditing purposes.

12. (Currently Amended) The PKI of claim 10 wherein the revocation protocol includes the certificate authority deleting the record representing the first ~~unsigned~~ certificate from the database.

13. (Currently Amended) A method of authenticating a subject to a verifier in a public key infrastructure (PKI), the method comprising the steps of:

issuing a first ~~unsigned~~ certificate from a certificate authority to the subject, the first certificate including ~~that associates~~ a public key of the subject, ~~to~~ long-term identification information related to the subject, and meta-data related to the first certificate, wherein the first certificate is not signed by the certificate authority;

maintaining, at the certificate authority, a database of records representing issued ~~unsigned~~ certificates that are valid until at least one of revoked by the certificate authority and expired;

storing a record representing the first ~~unsigned~~ certificate in the database;

maintaining, at the verifier, a hash table containing cryptographic hashes of valid ~~unsigned~~ certificates corresponding to the records stored in the database and including a cryptographic hash of the first ~~unsigned~~ certificate;

presenting the issued first ~~unsigned~~ certificate from the subject to the verifier for authentication;

demonstrating, by the subject, that the subject has knowledge of a private key corresponding to the public key in the ~~unsigned~~ first certificate.

14. (Currently Amended) The method of claim 13 wherein the first ~~unsigned~~ certificate includes an expiration date/time.

15. (Currently Amended) The method of claim 13 wherein the first ~~unsigned~~ certificate does not include an expiration date/time.

16. (Original) The method of claim 13 further comprising the step of:

storing the private key in a smartcard accessible by the subject.

17. (Original) The method of claim 13 further comprising the step of:

storing the private key in a secure software wallet accessible by the subject.

18. (Currently Amended) The method of claim 13 further comprising the step of:

computing, by the verifier, the cryptographic hash of the first ~~unsigned~~ certificate with a collision-resistant hash function.

19. (Original) The method of claim 18 wherein the collision-resistant hash function is a SHA-1 hash function.

20. (Original) The method of claim 18 wherein the collision-resistant hash function is a MD5 hash function.

21. (Currently Amended) The method of claim 13 further comprising the step of:

revoking the first ~~unsigned~~ certificate when ~~the association of the subject's public key to~~ at least a portion of the long-term identification information related to the subject ~~becomes invalid~~no longer applies to the subject.

22. (Currently Amended) The method of claim ~~21 wherein the revoking step includes the steps of~~13 further comprising revoking the first certificate when at least one of the private key is comprised and at least a portion of the long-term identification information related to the subject no longer applies to the subject, the revoking including:

retrieving the record representing the first ~~unsigned~~ certificate from the certificate database and obtaining a cryptographic hash of the first ~~unsigned~~ certificate;

sending a message from certificate authority to verifier containing the cryptographic hash of the first ~~unsigned~~ certificate;

requesting that the verifier remove the corresponding cryptographic hash of the first ~~unsigned~~ certificate from its hash table;

removing the cryptographic hash of the first ~~unsigned~~ certificate from the hash table;

notifying the certificate authority that the cryptographic hash of the first ~~unsigned~~ certificate is removed from the hash table; and

collecting, at the certificate authority, the notification sent in the notifying step.

23. (Currently Amended) The method of claim 22 wherein the revoking step further includes:

marking the record representing the first ~~unsigned~~ certificate in the database as being invalid, for auditing purposes.

24. (Currently Amended) The method of claim 22 wherein the revoking step further includes:

deleting the record representing the first ~~unsigned~~ certificate from the database.

25. (New) The PKI of claim 1 wherein the meta-data includes at least one of a serial number of the first certificate and a name of the certificate authority.

26. (New) The PKI of claim 1 wherein the long-term identification information related to the subject includes at least one of the subjects' name and a number identifying the subject.

27. (New) The PKI of claim 1 wherein the certificate authority and the verifier operate to revoke the first certificate when the private key corresponding to the public key in the first certificate is compromised.

28. (New) The method of claim 13 further comprising:

revoking the first certificate when the private key corresponding to the public key in the first certificate is compromised.